Changes Coming to DOD's Cybersecurity Maturity Model Certification under CMMC 2.0

Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

November 23, 2021

On November 17, 2021, the U.S. Department of Defense (DOD) published an Advanced Notice of Proposed Rulemaking (ANPRM) previewing significant changes to its Cybersecurity Maturity Model Certification (CMMC) program.[1] The revamp, "CMMC 2.0," promises a more streamlined and flexible system for defense contractors and their suppliers to comply with CMMC and DOD's cybersecurity expectations, with practical changes coming into effect between 9 and 24 months from now. CMMC 2.0 is DOD's response to a months-long internal review spurred by more than 850 public comments in response to DOD's September 2020 "CMMC 1.0" interim rule (see our webinar coverage of this rule here). While DOD pursues the forthcoming rulemakings, it intends to suspend current CMMC piloting efforts and has stated it will not include CMMC requirements in DOD solicitations. Contractors should continue, however, to adhere to the existing cybersecurity "assessments" framework (described here), focusing on compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 controls and required Basic Assessments.

Overview: Three-Tiered Model Based on NIST Controls

CMMC 2.0 will replace the five-level model of CMMC 1.0 with three progressively more complex levels of cybersecurity requirements, each keyed to independently established standards (e.g., Federal Acquisition Regulation (FAR) requirements, NIST requirements). The new model will also increase oversight of third-party assessors and eliminate all "maturity" requirements and CMMC-unique practices.[2]

Controls and Requirements

The new tiered requirements in the three-level model are as follows:

- *Level 1 "Foundational"* – Level 1 remains largely the same as in the prior model, with annual self-assessments and certifications by company leadership. Level 1 requires the same 15 controls, derived from FAR 52.204-21 "basic" controls required for protection of Federal Contract Information.
- *Level 2 "Advanced"* –
  - Level 2 in CMMC 2.0 is based on the old CMMC "Level 3," with a bifurcation of "prioritized acquisitions" and "non-prioritized acquisitions" in relation to the sensitivity of Controlled Unclassified Information (CUI) involved. As an example,

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+ 1 214.969.2713

Michael J. Vernick
Partner
mvernick@akingump.com
Washington, D.C.
+ 1 202.887.4460

Angela B. Styles
Partner
astyles@akingump.com
Washington, D.C.
+ 1 202.887.4050

Scott M. Heimberg
Partner
sheimberg@akingump.com
Washington, D.C.
+ 1 202.887.4085

Chris Chamberlain
Associate
cchamberlain@akingump.com
Washington, D.C.
+ 1 202.887.4308

prioritized acquisitions may involve CUI related to weapons systems, whereas nonprioritized acquisition might involve CUI related to military uniforms, though details on prioritization are expected in forthcoming rulemakings.

  - Prioritized acquisitions will require an independent third-party assessment from a certified third-party assessing organization (C3PAO) every three years, while nonprioritized acquisitions will require only an annual self-assessment and certification.
  - CMMC's new Level 2 reduces the number of required controls to the 110 controls included in the NIST's SP 800-171 Rev. 2 (NIST SP 800-171), thereby eliminating what are now 20 additional Level 3 CMMC 1.0 controls.

- *Level 3 "Expert"* – CMMC's new Level 3 will replace existing Levels 4 and 5. Most notably, acquisitions at this level will require triennial **government-led** assessments (i.e., not by C3PAOs). Further, in addition to the 110 controls required for new Level 2, Level 3 certification will also require compliance with the controls in NIST's SP 800-172. The decision to equate Level 2 and 3 controls with NIST standards is especially notable in relation to other efforts by the Biden administration to centralize further NIST's role in federal cybersecurity, including under E.O. 14028 (discussed here).

MODEL		ASSESSMENT	CMMC Model 1.0
171 practices	**5** processes	**Third-party**	**LEVEL 5** ADVANCED *CUI, critical programs*
156 practices	**4** processes	**None**	**LEVEL 4** PROACTIVE *Transition Level*
130 practices	**3** processes	**Third-party**	**LEVEL 3** GOOD *CUI*
72 practices	**2** maturity processes	**None**	**LEVEL 2** INTERMEDIATE *Transition Level*
17 practices		**Third-party**	**LEVEL 1** BASIC *FCI only*

CMMC Model 2.0	MODEL	ASSESSMENT
LEVEL 3 Expert	**110+** practices based on NIST SP 800-172	Triannual government-led assessments
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	Triannual third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	**17** practices	Annual self-assessment

Graphics recreated from U.S. Department of Defense Office of the Under Secretary of Defense Acquisition and Sustainment CMMC website: https://www.acq.osd.mil/cmmc/about-us.html

The ANPRM states that the new CMMC 2.0 framework will be implemented by a pair of rules in both Title 32 (National Security) and Title 48 (FAR and Defense Federal Acquisition Regulation Supplement (DFARS)) of the Code of Federal Regulations (CFR), and that each will be open for public comment.

POAMs and Waivers

In a notable departure from CMMC 1.0, the DOD will allow some acquisitions to satisfy requirements via plans of action and milestones (POAMs) (i.e., in lieu of actual compliance) under CMMC 2.0. Specifically, in limited circumstances, contractors with POAMs will be able to receive some contract awards while they make progress toward full compliance. DOD will not, however, accept a POAM for certain "high[ly] weighted" controls. Moreover, a company seeking to meet CMMC 2.0 requirements through a POAM must achieve a certain minimum threshold score.[3] Further, eligible contractors must complete POAMs within 180 days of contract award after which a contracting officer may terminate the contract if controls have not yet been implemented.

In addition to POAM's, CMMC 2.0 will also introduce the concept of waivers for certain mission-critical work. Such waivers will be strictly time-limited and may only be approved by senior DOD personnel.

Takeaways

DOD's proposal is responsive to concerns raised by the defense industrial base in several ways, including its simplification of five levels into three, a greater reliance on existing federal sources of cybersecurity guidance (i.e., NIST standards), and—at least in some circumstances—continued allowance of self-attestations of compliance by many defense contractors. At the same time, DOD's renewed model comes on the heels of aggressive efforts to strengthen cyber and supply chain security across the federal government under the Biden-Harris administration's E.O. 14028 (May 12, 2021) (discussed here), as well as the administration's further empowerment of NIST and the Cybersecurity and Infrastructure Security Agency (CISA) in those efforts. Further, against backdrop of the Justice Department's cyber-fraud initiative (discussed here), DOD's simplification of CMMC requirements and the retention of self-attestation elements increases the risk of False Claims Act (FCA) enforcement for government contractors.

DOD's approach to CMMC 2.0 through an ANPRM signals its desire to supply industry with opportunity for engagement and early preparation for its forthcoming rules and subsequent requirements. In the meantime, defense contractors and their suppliers should continue to adhere to the existing cybersecurity "assessments" framework (described here), focusing on compliance with NIST SP 800-171 controls and required Basic Assessments. In related releases, DOD indicated its plans to release updated assessment guides for CMMC 2.0 Levels 2 and 3 by the end of November, which we expect to closely track NIST guidance.

[1] *Dept. of Defense, Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, Advanced Notice of Proposed Rulemaking* (November 8, 2021).

[2] *Id*. at 3.

[3] Dept. of Defense, *CMMC Implementation*, Acquisition & Sustainment, available at https://www.acq.osd.mil/cmmc/implementation.html#impHero.